Commonwealth of Massachusetts
Information Technology Division

Enterprise Wireless Security Standards: Wireless Mobile Communications Version 1.1

This document identifies standards to ensure secure deployment, use and administration of Wireless Mobile Communications (WMC) by Commonwealth entities. Entities considering deployment of these technologies should first consult the Enterprise Wireless Security Policy. Entities covered by this policy must adhere to the standards detailed in this document for all WMC deployments.

This document is one of the following Enterprise Wireless Security Standards documents that address major categories of wireless technology implementation:

- Wireless Mobile Communications (WMC)
- Wireless Local Area Networks (WLAN)
- Wireless Personal Area Networks (WPAN)
- Wireless Wide Area Networks (WWAN)

Additional references that entities may find useful as they plan WMC deployments are listed at the end of this document.

Wireless Mobile Communications (WMC)

Wireless Mobile Communications utilize licensed frequencies for data communications through such services as 2G and 3G cellular telecommunications, Cellular Digital Packet Data (CDPD), Global System for Mobile Communication (GSM), and General Packet Radio Services (GPRS), among others. Wireless mobile devices include RIM Blackberry, iPAQ and other PocketPC or PalmOS handheld devices, laptop and tablet computers using wireless mobile communications cards for data communications, and Internet-enabled phones. Commonwealth security standards for wireless mobile communications are based upon industry standards, National Institute of Standards & Technologies (NIST) security guidelines, and existing Commonwealth policies on IT Security and Remote Access. Both users and devices must be authenticated in order to access Commonwealth networks and information resources using wireless mobile communications.

1. Infrastructure Standards (WMC)

A. Untrusted Remote Access Networks
Wireless mobile communications are vulnerable and must be treated like untrusted remote access networks rather than members of an internal (i.e., MAGNet) trusted network.

Please Note: Commonwealth entities must ensure that wireless users cannot bridge wired and wireless LANs by disabling default-bridging capability in devices.

B. Ensuring network availability, reliability and support

Entities should develop policy-based network availability and reliability for high-priority traffic (e.g., for wireless mobile communication for emergency notification) requirements; entities or their network providers should establish requirements for Help Desk and support coverage (e.g., 24x7), maximum time to respond for service calls, service reliability (e.g., Mean Time Between Failures), network coverage, and maintenance of software and equipment at current firmware/software revision levels.

C. Monitor network security and performance
Entities should develop the capacity to effectively manage their wireless network segments and applications, including monitoring wireless network traffic, devices and potential security risks. Intrusion detection/prevention capability is recommended for complex networks.

2. Authentication & Encryption Standards (WMC)

Commonwealth entities must confirm that all communications between wireless and wired networks include both user authentication and data encryption by using one of the methods identified in Section 2. “Authentication & Encryption Standards,” and Section 3. ”Device Configuration and Security Standards.”

A. No unauthenticated access allowed on LAN/MAGNet
Unauthenticated public access is not allowed on the Commonwealth LAN or MAGNet network. Any LAN that allows unauthenticated access must be separated from the LAN/MAGNet and treated as a separate DMZ external to the secure network. In order to access LAN/MAGNet resources, devices must utilize an ITD-approved VPN solution (e.g., SSL and IPSEC) to protect transmissions end-to-end and must use two-factor authentication (e.g., certificate and password; SecureID card and password, etc.). Any access to the LAN/MAGNet from such a network must comply with the Commonwealth’s Enterprise Remote Access Security Policy.

B. Encryption within applications required
Entities must be aware that outward facing applications (e.g., customer and vendor programs) may be running across insecure wireless networks at the customer or vendor site. Entities must design such applications to enforce data security through encryption at the application level (for example, SSL 128-bit encryption within browser for e-mail, or SSL web interface to customer facing systems). All such applications, whether for PC, PDA, or SmartPhone, must support Internet browser with a minimum SSL128-bit encryption (or equivalent for non-web applications).

C. Local caching, storing and printing
Entities must be aware that local storing, caching or printing of confidential data on remote devices may pose a significant data security risk. Entities must advise users that confidential data as defined by the entity cannot be stored on the devices unless strongly encrypted. Entities must develop local policy as required to address this potential risk, in compliance with the Commonwealth’s enterprise security policies as published by ITD, and relevant data confidentiality acts such as HIPAA, FIPA, or FERPA, based on the type of data involved.

D. Registration of devices

Entities must require registration of each wireless device prior to the device being admitted and/or connected to the entity's LAN. Serial numbers, phone numbers, MAC address, etc., as appropriate and obtainable for each wireless communications device, must be recorded. This information must be made available to ITD upon request.

3. Device Configuration and Security Standards (WMC)

The portability and opportunity for loss/misplacement/theft of wireless mobile communications devices mandates that strong measures be utilized to protect any data on the devices as well as the devices themselves.

A. Protection of connected devices
All wireless mobile communications devices that connect to the Commonwealth LAN/MAGNet must be configured in compliance with the Commonwealth's Enterprise Security Policies, Standards and Procedures as published by ITD. Devices must be fully updated and patched, and must run personal firewall and anti-virus software, if available for the device, in compliance with the Commonwealth and Commonwealth entity's policies.

B. Ownership of connected devices
All wireless mobile communications devices that connect to the Commonwealth LAN/MAGNet must be the property of the Commonwealth. No personally owned wireless mobile communications devices or vendor equipment may connect without express written permission of the Executive Department CIO, subsequent to a recommendation from the Enterprise Security Board. Entities may apply for variances to this ownership requirement on an application-specific basis.

All users of wireless mobile communications devices must complete and sign a user acceptance agreement, similar to the current Virtual Private Network (VPN) user acknowledgement, allowing ITD and their Commonwealth entities to scan/monitor mobile communications devices during connection attempts to LAN/MAGNet resources and throughout the connected session. The user acknowledgement form must state that no one other than the authenticated user can use the device. Users of non Commonwealth-owned devices who have been approved for such use by the Executive Department CIO must complete the same user agreement noted above.

C. Administrative control of connected devices
It is required that the entity maintain exclusive administrative control of the configuration of all wireless mobile communications devices directly connected to the LAN/MAGNet, to ensure that the device is free of viruses and that the operating system/firmware is regularly updated.

D. Authentication of connected devices
Connected devices must have a first tier authentication for device access – either a password or PIN (personal identification number), or equivalent, such as a biometric (fingerprint scanner), voice recognition, etc. This first tier authentication helps to protect any data physically stored on the device. In order to access LAN/MAGNet resources, devices must utilize an ITD-approved VPN solution (e.g., SSL and IPSEC) to protect transmissions end-to-end and must use two factor authentication – (e.g., certificate and password; secureID card and

password, etc.). Any browser-enabled devices must use, at minimum, SSL 128bit encryption technologies.

E. Wireless carriers for connected devices
Connected wireless mobile devices must be subscribed to a wireless carrier/provider that is currently listed on ITT09, the Commonwealth's statewide contract for wireless cellular communications services. No devices will be allowed to authenticate to any Commonwealth LAN/MAGNet system unless the carrier/provider is in active standing with the Commonwealth Operational Services Division (OSD).

F. Physical security of remote devices
Entities must develop policies regarding the physical security of wireless mobile communications devices, including procedures to prevent theft or loss and to report theft or loss in the event of such occurrence. Entities and their wireless service providers should establish procedures and acceptable response times to terminate access from lost or stolen devices. Entities must advise users that confidential data, as defined by the entity, cannot be stored on wireless mobile communications devices.

Additional Reference

National Institute of Standards and Technology (NIST) Special Publication 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices", by Tom Karygiannis and Les Owens, November 2002.